(C) 2003 Airscanner Corp. http://www.airscanner.com

Airscanner Mobile Sniffer

For Windows CE / Pocket PC

Technical Whitepaper and User's Guide

Level:
___ Beginner
_x_ Intermediate
_x_ Advanced
___ Expert

Estimated Reading Time: 60 minutes

(C) 2003 Airscanner Corp. http://www.airscanner.com

Sniff passwords from your Pocket PC

As a network administrator, you want to protect your users' confidential data. What better way to do this than to stroll down the hall with Airscanner(TM) Mobile Sniffer hidden in your pocket? Thanks to our **support for Ethereal** packet capture format, grabbing your user's passwords out of the airwaves is as easy as watching a movie! Your users unintentionally send their passwords through the air in clear text, so it is better that you discover this first before a malicious drive-by hacker does it for you. Airscanner(TM) Mobile Sniffer also **works in promiscuous mode**, so you can also discover unauthorized users who may be associating with one of your access points.

Audit WLANs from your PDA

Are you tired of dragging your laptop all over campus to audit your WLAN? Simply slip Airscanner(TM) Mobile Sniffer into your pocket, and you are ready to go. Airscanner(TM) Mobile Sniffer packs the power of a full-scale sniffer into an application for portable devices. Once your Windows CE device is linked to the network, Airscanner(TM) Mobile Sniffer monitors all activity within a given segment. Airscanner(TM) Mobile Sniffer also allows you to **set your own filters**, allowing you to monitor only the information you need.

Features

Airscanner(TM) Mobile Sniffer gives you the power to:

- Sniff wireless packets in promiscuous mode
- Decode UDP, TCP, Ethernet, DNS, and NetBios packets
- Conduct network analysis on an entire WLAN segment
- Customize filters for source and/or destination IP Address, UDP Port, TCP Port, or MAC
- View real-time packet statistics
- Save results of capture sessions
- Export data to Ethereal format for further analysis on a desktop PC

Benefits

Airscanner(TM) Mobile Sniffer advantages include:

- True promiscuous wireless sniffing
- Works on most Pocket PC devices
- Supports a broad range of wireless network cards
- Free for home or personal use
- World class customer support for commercial licenses
- Crystal-clear network analysis thanks to Ethereal format support

(C) 2003 Airscanner Corp. http://www.airscanner.com

Requirements:
Windows CE device running PocketPC 2002
Compatible wireless card

Licensing:
-- Free for personal (non-commercial) use.
-- Corporate, Educational, Government, and Small Business/Home Office users must purchase an annual license within 30 days of installing the software

(C) 2003 Airscanner Corp. Please ask permission before redistributing this software or user's manual

Version History

Version 1.0 released April 30, 2003

Version 1.02 released May 7, 2003

- Included support for Toshiba e740 series and IPAQ 5450 Series (see FAQ and the end of this document)

- Minor Bug Fixes

Note: The following document is more than a user's manual; it is also our attempt to help educate you on the science of sniffing. We hope you will take the time to read this entire manual so that you will be better equipped to defend yourself and to audit your own wireless networks.

1. Overview

When the typical end user sends an instant message to their friend or family member on the other side of the world, not much thought is given to the technology that makes it happen. To them, they simply type the message in a window and when they hit the *Enter* button, the message is magically transported to their friend's screen. While this appears to be an instantaneous relay of data, in reality the message passes through a legion of interconnected hardware devices that process the data before it arrives at its destination.

Although it seems easy, the technology responsible is very complex and requires an in depth understanding of communication protocols and how they are used by hardware devices to pass and control data flow. A network administrator must understand the use of hubs, switches, routers, TCP/IP, SMB and more in order to audit or debug network communication. This brings us to the sniffer.

A sniffer is merely a data collection tool that allows its user to see what data is passing on a network. This tool can come in the form of a simple software program included with an OS (e.g., Windows Network Monitor, AIX iptrace) or as part of a complex and very expensive hardware device (e.g., $40,000 GTX Multi-protocol analyzer) that can handle multiple network lines and GBs of data. Though it is just a tool, it, like many other simple tools, can be used for good or evil. For example, a sniffer can help an administrator find a malfunctioning network card, just as easily as it can help a malicious hacker monitor network traffic for user names, passwords, or other sensitive data that could be abused to gain unauthorized access to a network.

This manual will describe how a sniffer works, and how it can be used to help you troubleshoot a networking problem. We will also demonstrate methods in which you can use a sniffer to troubleshoot applications that require network access to function. In addition to these legitimate purposes, we will also illustrate how a hacker can abuse a sniffer to gain access to private information. Hackers already know how to do this, so it is imperative that you learn their attack methods so that you can properly protect your networks.

2. Sniffer Fundamentals

As previously mentioned, a sniffer allows you to view and analyze raw network traffic. This traffic can be on a wire, fiber line, or even in the air on a wireless network. While the data typically flows flawlessly from one point to another, there are times when something goes wrong and a technician or administer needs to get inside the traffic to see what is happening. However, this is not as easy as plugging in a computer and collecting data. As we will

demonstrate, sniffing a network properly take a solid understanding of how the various pieces of equipment and software work together in unison.

2.1 Requirements

Sniffing a network is not as simple as plug and play. There are several requirements that must be met before a sniffer will operate, depending on the target data. This section will outline the technical aspects of network sniffing and the necessary hardware and software components needed to successfully capture data.

2.1.1 Hardware

Before you attempt to sniff, you must have the proper hardware. This is not as simple as selecting any network card off the shelf and plugging it in to a computer and expecting it to work. Due to compatibility issues with the OS, other hardware components, and more, it is important to perform some preliminary research into a sniffer's requirements before purchasing anything.

One particular area where the right hardware matters is when attempting to sniff a wireless network. This is because there are several major types of wireless network cards (WNICs) available on the market. For example, you can currently buy 802.11b, 802.11a, 802.11a/b, 802.11g/b cards and even 802.11a/b/g cards. In addition, within just the 802.11b group (the most popular group) there are two main types of chipsets that are used on the WNICs: *PrismII* and *Orinoco*. Therefore, you will want to investigate the product and its hardware requirements, in addition to the network

2.1.2 Drivers

Once you have the appropriate hardware, you still need to ensure that your OS has the right drivers to use that hardware. This can be a tricky part of getting a sniffer to work properly, and it is why many sniffers either run on Unix based OSs, or require a special driver to be installed before it will work in Windows.

In the case of the mobile Windows environment, most general-purpose *local* sniffers will work with any WNIC without the need for a special driver or patch. Assuming your WNIC is working before a sniffer is installed and the sniffer program is compatible with your card, you will need no extra drivers. This said, if you want to perform wireless sniffing, your sniffing *will* be limited. Currently there are no publicly available drivers that make true promiscuous sniffing a reality for the Pocket PC. Instead, you will only have access to networks with which your WNIC can associate, and then with only one at a time.

Note: If you are installing a Windows sniffer, you will probably need a special driver known as Winpcap available at http://winpcap.polito.it. To install this driver, simply download and double-click the executable. The installation process is straightforward and only requires a few clicks of your mouse.

Note: Airscanner Mobile Sniffer™ is based in part on Winpcap, so you will not have to install Winpcap separately as Airscanner Mobile Sniffer™ will install the necessary parts for you. However, you will need to install it if you plan to use Ethereal for advanced post-data capture analysis (recommended).

Installation of a sniffer on Linux usually requires no extra drivers other than those required for normal operation. The only exceptions to this are wireless sniffers, which require patches or a special driver. Ensure you read the sniffer's documentation before installation to avoid hours of frustration.

2.1.4 Promiscuous Mode

When a network card is manufactured, it is assigned a unique identifier known as a Media Access Control (MAC) address. Since this address is supposed to be unique, is serves as one of the fundamental methods by which data is transmitted over a network. While there are many other communication protocols that sit on top of the MAC address to help with data flow, the MAC address is used in the first and last leg of the transmission process. It is important to understand the importance of the MAC address, because it indirectly affects what data a sniffer can access.

When a network card is operating normally, it actually scans each packet of data traveling over the network to see if any of the data is labeled with its MAC address. If there is a match, the data is passed up to the next layer in the protocol stack, and ultimately to the program to which it was sent. However, if the packet is not addressed to the NIC, it will be ignored.

Since the sniffer software actually operates above the hardware layer of the communication stack, it will only receive data that was sent to the computer on which it is operating. In other words, the sniffer will only see local data. While this level of access can be helpful in some situations, the limited access will restrict most troubleshooting efforts. However, this is where promiscuous mode comes into play.

When a network card is placed in promiscuous mode, it will accept ALL data passed on the wire to which it is connected, regardless of any MAC address. However, there are still some obstacles a sniffer must overcome to gain access to network traffic. This includes additional support for wireless data, which uses radio waves to pass data, and limitations due to networking technology.

2.2 Switches and Hubs

Within any local area network you will find network hubs and/or switches. These devices are very similar in appearance, and on the surface perform the same duties. However, once you look at how these devices work, you will quickly see that they are inherently different devices.

A hub is a very simple *passive* device that receives data in on one port and distributes it to all the other ports. It does not examine or care what data passes through it, nor does it care where the data ends up. While hubs have been inexpensive for a long time due to their relative lack of "intelligence", which requires more circuitry and programming, they are often slower and can produce overload conditions when three or more hubs are connected together because all data is passed to the entire network. Although this can cause bottlenecks and network saturation, a hubbed network is the best type of network in which to place a sniffer. Since hubs do not restrict data in any way, a sniffer will have access to ALL the data flowing across the wires and through the hub.

A switch, on the other hand, is an *active* device. It records the MAC addresses of each network card to which it is connected and creates an internal table of MAC to IP address rules to help control traffic flow. In other words, a switch will examine each packet header for a matching IP address. Once a match is found, the switch will pass the data to the port with the corresponding MAC address. Note, it will pass data only to the port which matches the IP/MAC table, which means any sniffer connected to another port on the sniffer will NOT have access to that data; at least, not without some network manipulation.

In the case of a wireless network, you could be dealing with several networking environments. This is because the wireless part of the network is similar to a hub due to the fact that data is sent out over the airwaves and there is no method to control who or what has access to it.

2.3 ARP Spoofing

As we have previously discussed, the existence of a switch in a network is a serious obstacle to a sniffer. Due to a MAC/IP table, traffic from one NIC will only be passed to the NIC to which it is addressed. However, it is possible to manipulate the network to successfully gain access to traffic passing on other ports. This is accomplished using a method known as ARP spoofing.

The Address Resolution Protocol (ARP) is used by network devices to establish a relationship between MAC addresses and IP addresses. This is to reduce the complexity of maintaining a network by providing an easier method of addressing that can be automated and more easily used. To speed up the process of this conversion, many network devices create an ARP table that temporarily stores recently received IP addresses and their corresponding MAC addresses. If an ARP entry is made between two devices, any further data transmissions do not need to perform another ARP request to determine the MAC address of the target device.

While the use of an ARP table speeds up the data transmission process, it also creates a huge hole that can be exploited by a sniffer. In short, an ARP table can be manipulated by sending spoofed ARP *Replys* to communicating network devices. In this network trick, the hacker will basically places his or her computer in the middle of an existing data path by creating false ARP entries in both the target's computer and the gateway device (or what ever computer with which the target is communicating). Once the hacker establishes himself in the middle, he can easily capture, record, or even change the data passing between two network devices.

2.4 Filters

A good sniffer is more than just a packet collection device or program. At its fundamental layer, a sniffer simply gathers data and stores it in a file, which can grow to be several gigs in size in only a few minutes, or hours on a slower network. While this data is exactly what a troubleshooter wants, it can quickly become overwhelming and can in effect swamp the user with too much irrelevant information. In other words, finding that one desired piece of information can be much like finding a needle in a haystack.

As a result, many sniffers have incorporated the use of filters to control and regulate the amount of, and type of, data that is collected and/or analyzed. If a sniffer uses a filter, data analysis can be easily narrowed down to just the information that is considered relevant to the job. In addition, if the filter is a pre-capture filter, it can significantly reduce the amount of irrelevant data that is captured, thus saving valuable time and resources that can become heavily taxed when collecting data for a long period of time.

There are many variations of filters available, which are represented by a filtering language. These languages can be proprietary, or based off a standard filter, such as the OFDM (Open Filter Definition Language). Regardless of the technical aspects of the filtering language, most filters are very similar in appearance and are easy to understand. The following represents two filters, one from Ethereal, which is the most common free sniffer available, and the other using the OFDM language.

Ethereal
udp.srcport == 67 or udp.srcport == 68 or udp.destport ==67 or udp.destport == 68

OFDM
(udpport(src) == 67 || udpport(dest) == 67 || udpport(src) == 68 || udpport(dest) ==68)

As this illustrates, filtering languages are basically a series of conditional statements. This example will filter all data for DHCP traffic, which can be detected due to its use of the UDP protocol and port numbers 67/68.

2.5 The right sniffer for the job

The quality of a sniffer is directly related to the information it can provide for its user. For example, many hackers consider dsniff to be one of the best sniffers available. This is not because dsniff captures any better than Ethereal, which is at the top of the list for many professionals; instead, it is because dsniff incorporates extra features, such as a built in password sniffer, arp spoofing technology, and more. These small additions make the program more streamlined, if collecting passwords is your goal. On the other hand, some troubleshooting will require the use of an expensive all-in-one hardware/software sniffer package. These devices, which would be overkill for a small network, can collect gigs of data and never miss a packet.

In addition to landline sniffers, the introduction of wireless networks has caused the creation of a whole new niche of sniffers. Due to the unique physical and technical properties of WLANs, the quality or functionality of a sniffer is tied to how well it can be integrated into an existing wireless network. Some sniffers will only capture packets from WLANs to which they are associated, while others can capture data on all operating networks within its physical proximity. For an 802.11b network, this is due to the fact that up to 14 different channels are used to transmit data. As a result, it is possible to have up to four different and totally separate WLANs in the same general area (several channels are used per network). To collect data from all local wireless networks, the wireless device on which the sniffer is operating would have to operate in a passive mode. While this would allow it to capture all data, the device would not be able to connect to any existing wireless network. In other words, it would be continuously jumping channels, which is similar to jumping networks several times a second. Due to the

nature of networking, this would wreck havoc on any attempted communication sessions. To make this even more complicated, sniffing a wireless network in passive mode requires special drivers, or at the minimum a patch to existing drivers.

3. Practical Sniffing

Now that you understand the many facets of sniffing, it is time to take a look at how you can benefit from Airscanner Mobile Sniffer™. In addition, we have included a section on Ethereal to help you prepare for future analysis of collected data from Airscanner Mobile Sniffer™. With Ethereal, you will be able to quickly analyze collected data and drill down on potential network problems.

3.1 Airscanner Mobile Sniffer™

URL: www.airscanner.com
Supported Platforms: Windows CE 3.0

3.1.1 Description

With the current trend toward mobile computing, Airscanner has released a sniffer potentially capable of operating on any PocketPC device that supports the use of a WNIC. This sniffer not only allows its user the freedom to roam independent of wires, but since it operates on a pocket PC, a user can sniff the airwaves from the palm of her hand. Using this sniffer is as easy as hitting one button, which will then start the sniffing process. Data is captured in Ethereal format, which is one of the most popular formats currently used by security professionals.

In addition to basic sniffing, Airscanner Mobile Sniffer™ includes a fairly robust filtering feature based on the OFDM language. With a filtering enabled, a user can quickly get access to the data that is most important to them. This eliminates the need to waddle through hundreds, if not thousands of packets just to locate a single byte of data. However, due to the limited screen size of most pocket PC devices and other usability issues that most mobile devices have, the ability to save and review packets in Ethereal makes Airscanner an excellent *peripheral sniffer* for any administrator.

3.1.2 Requirements

The Mobile Sniffer does have several requirements before it will run correctly. These include the following:

- Pocket PC operating system.
- Installation of operational wireless network adapter.
- Installation of proper drivers.

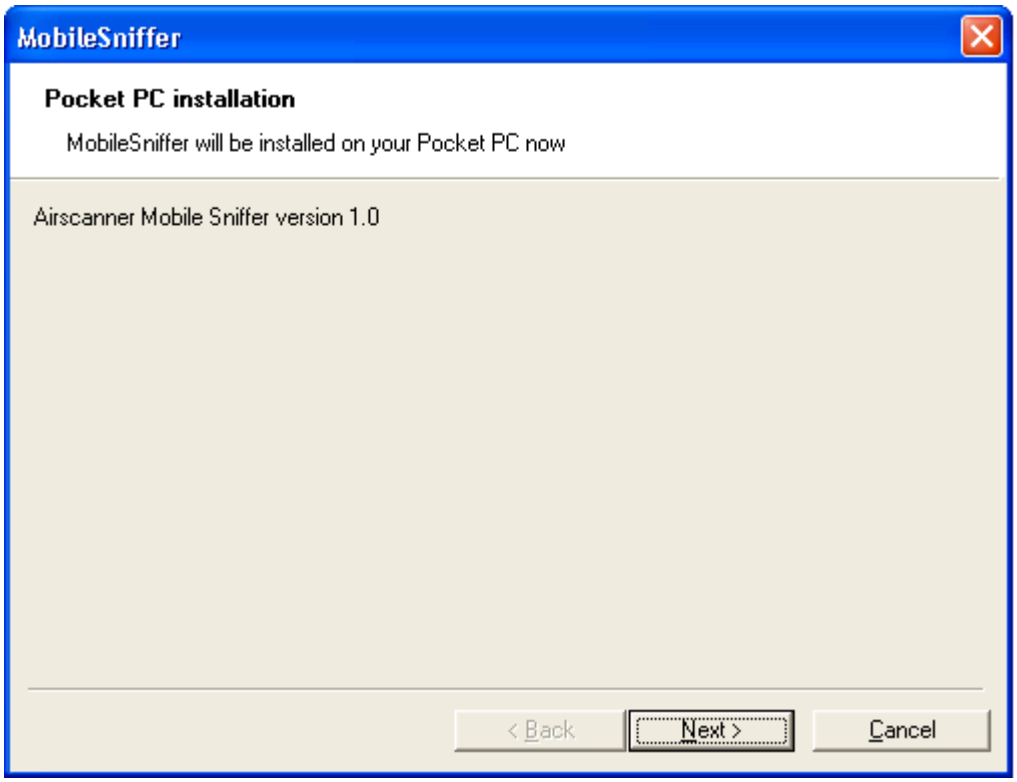
If any of these items are not met, Airscanner Mobile Sniffer™ will not install, or it will run incorrectly. Symptoms of a problem include obvious error messages, program crashes, or the lack of promiscuous mode during an otherwise normal sniffing session. If you do have a problem, be sure to verify that your wireless network card is a Prism2 based card and that you have the correct and intended drivers for your WNIC (e.g., improperly using a Linksys WPC11

v1.1 card with Compaq's WL100NDS.dll driver may not work).

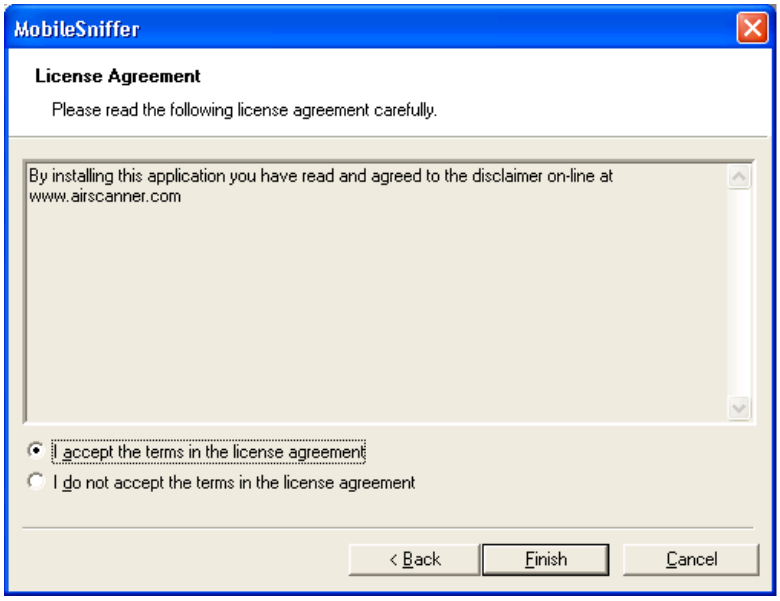
3.1.3 Installation

Assuming you have met all the requirements, installation is a straightforward process. Follow the instructions provided and you should be scanning the airwaves in no time at all.

1.Download Airscanner Mobile Sniffer™ to your local PC
2.Sync your pocket PC device to your computer
3.Double click the Airscanner Mobile Sniffer™ setup .EXE
4.Click the [Next] button



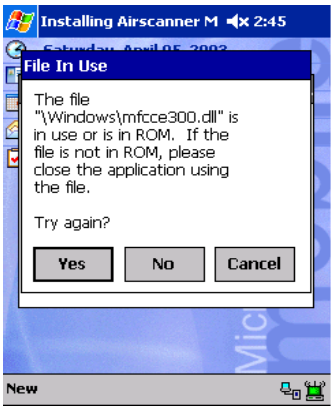
5.Review the license and click [Finish] if you agree. By using this product you have read and agreed to the legal disclaimer and license requirements posted on www.airscanner.com.

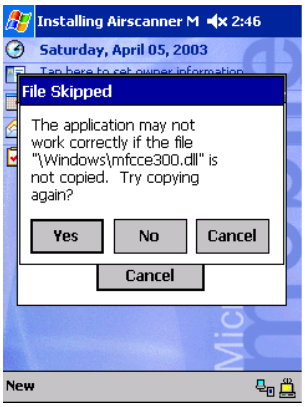

MobileSniffer
License Agreement
Please read the following license agreement carefully.
By installing this application you have read and agreed to the disclaimer on-line at www.airscanner.com
I accept the terms in the license agreement
I do not accept the terms in the license agreement
< Back
Finish
Cancel

6.MobileSniffer is the default install folder (unless you want to store the files elsewhere)
7.Click [OK] once the program is done installing

Application Downloading Complete
Please check your mobile device screen to see if additional steps are necessary to complete this installation.
OK

8. **Important:** On the pocket PC device, if you are warned about overwriting mfcce300.dll file, click the [No] button twice. If this file already exists on your, you do not need to overwrite it with another.


Installing Airscanner M 2:45
File In Use
The file "\Windows\mfcce300.dll" is in use or is in ROM. If the file is not in ROM, please close the application using the file.
Try again?
Yes
No
Cancel
New



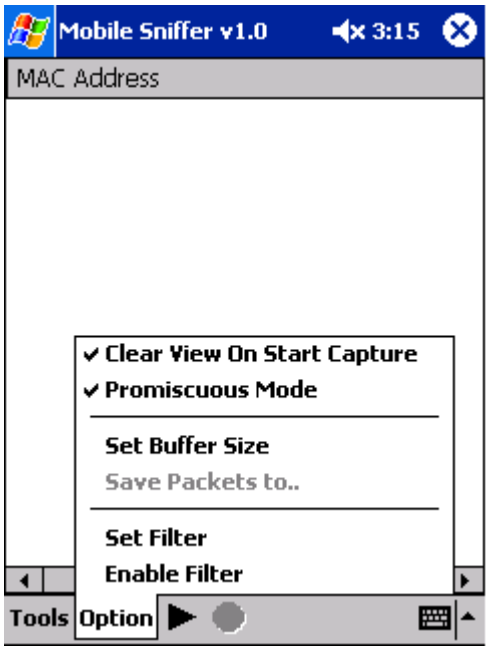
3.1.4 Using Mobile Sniffer

The following will outline the usage features of Airscanner Mobile Sniffer™. It assumes you have Airscanner Mobile Sniffer™ installed and working properly (i.e., with the correct drivers).

To use Airscanner Mobile Sniffer™, locate the MobileSniffer icon in your start menu and select it. After clicking it, you will see an adapter selection screen listing the network adapters that are installed on your pocket PC. Select the appropriate adapter from the list, and click [OK]. At this point you are actively sniffing and you could soon see collected packets begin to appear on the screen.

3.1.5 Menus

Airscanner Mobile Sniffer™ is laid out in a functional and logical format. There are two menu options on the menu bar at the bottom of the pocket PC window, which also includes a [Play] button and a [Stop] button. The following will include a break down of the menu options and what they are used for.



3.1.5.1 Options Menu

This menu is used to control and set the various operational configurations. Included are filter settings, buffer sizes, and capture mode.

Clear View on Start Capture

This option determines whether or not you want the screen to append new captured data to existing information or if you want the screen to clear before listing any new packets. If selected, your screen will clear, which could erase information you wanted to review. This option was included to let you make the decision if you wanted the old data erased or not. It is set by default to clear the screen at the start of each capture session.

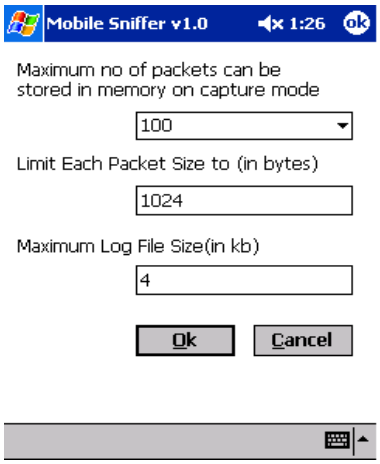
Promiscuous Mode

A sniffer can operate in two different modes: promiscuous or non-promiscuous (see the

previous overview of promiscuous mode for more information about this mode). Typically, you will want to operate in promiscuous mode, which is selected by default. However, if your WNIC doesn't support promiscuous mode, or if you are only concerned with the data traveling to and from your device, you can select this option to only capture *local* traffic.

Set Buffer Size

The Airscanner Mobile Sniffer™ buffer size refers to the storage settings used when sniffing data. Due to the limited space, special consideration must be paid to the amount of information that is captured. By selecting this option, you will gain access to three main properties of data collection that can help you save space and narrow down the information you are actually collecting.



The first option is the number of packets to collect. This is set at a default of 100 packets. This is a conservative setting, but we prefer to allow you to increase this setting to a higher value as your Pocket PC device permits. If it is too high, you could quickly fill up all spare space in your Pocket PC device. The second option, Packet Size Limit, was added to allow you to focus only on header information. If you aren't concerned with the data in the packet, this setting can be decreased to a lesser value, which will simply cut off any data over the limit. Due to the specifications of the 802.11b standard, the maximum packet size is approximately 1500 bytes, which is reflected in the default setting. The final setting, max log size, simply defines the maximum amount of space to be used to store collected data. Again, the default 4kb is a conservative amount, so you will want to increase this to an amount relative to the space you have available.

Save Packets to…

This option defines the location where you can save the collected data. If you have an external memory resource, such as a CompactFlash card, you can elect to store the data on the CF card, instead of on the local RAM.

Set Filter

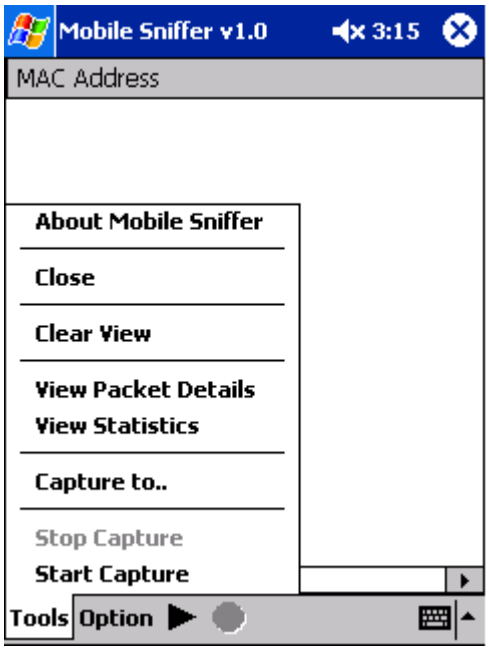
This option allows you to access the filtering part of Airscanner Mobile Sniffer™. This option is covered in detail in the filtering section.

Enable Filter

By default, filtering is not enabled when sniffing. However, if you want to narrow down the collected data to an exclusive protocol or device, you can use a filter. This option provides you with a quick method of enabling and disabling filtering.

3.1.5.2 Tools Menu

The tools menu is focused on the operational functions of the Mobile Sniffer. In this menu, you can gain access to packet and traffic details, and more.



About Mobile Sniffer

Selecting this menu will present you with general Airscanner information, and the version of Airscanner Mobile Sniffer™. This will be one of the first places you will be asked to go when requesting support.

Close

Closes the program view.

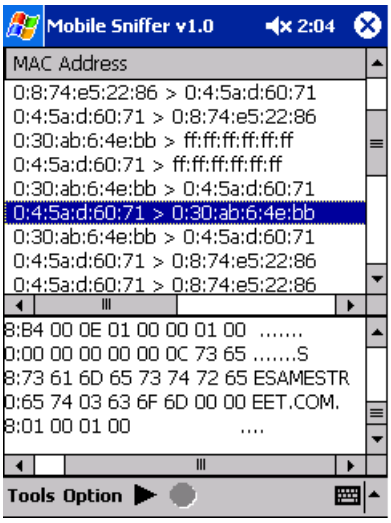
Clear View

After a session, your screen will be filled with information about the packets you collected. This option clears that screen and resets the capture files.

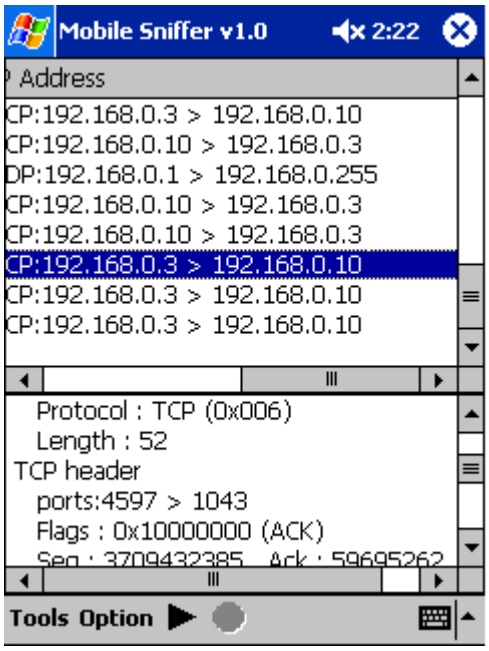
View Packet Details

While knowing the IP address and MAC address of each packet is useful, the real power of sniffing is knowing what is inside the packet. This option gives you the ability to peek inside the packet to see what data is actually passing via the airwaves. In the following screenshot, by using Airscanner Mobile Sniffer™ we can see that one person on the WLAN is accessing a website.

(C) 2003 Airscanner Corp. http://www.airscanner.com

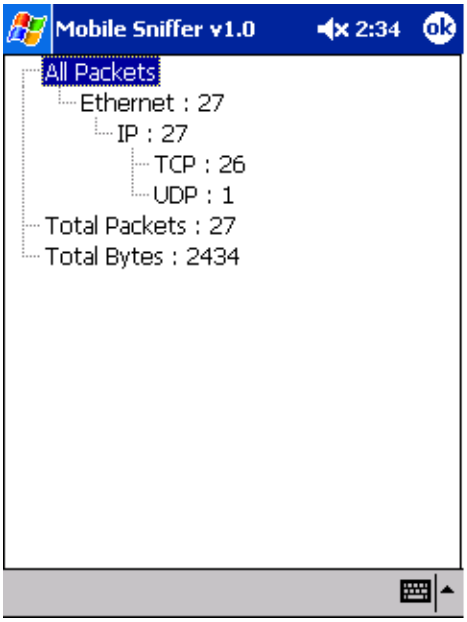


The details also include all of the information about the actual packet. Items such as time, length, MAC address, IP address, IP version, protocol, ports, packet flag status, sequence number and more are listed for your inspection. Note: While viewing details, you cannot operate in sniffer mode.



View Statistics

To help see the big picture, Mobile Sniffer includes a statistics tool that provides its user with a breakdown of the type of packet collected and total amount of data collected. This screen will help you determine how close you are to meeting your maximum buffer size, as well as giving you a rough snapshot of what type of data is passing over the network.



Capture to…

This option allows you to define where on the pocket pc you want to save the capture file. Like the 'Save Packets to..' option, this will help you control where to store data to avoid overflowing the pocket pc's device.

Start/Stop Capture

In addition to the Start/Stop buttons on the Menu bar, you can also start and stop the program from the Tools menu.

3.1.6 Filtering

Airscanner Mobile Sniffer™ includes a simple filter that will allow you to define the data collected. This will reduce file sizes and will help narrow down the collection to just the data that is of interest. Since you can easily import the collected data files into Ethereal, enhanced filtering is not necessary.

The filtering page allows you to define a maximum of two filters. The filters are defined as the following:

- Protocol: TCP, UDP
- MAC Address: The hardware address of a WNIC. Existing MACs will be displayed in the capture window. This can help you collect data from a particular client, regardless of their IP address.
- IP Address: The IP address assigned to the WNIC. Existing IPs will be displayed in the capture window. This can help you target a particular client from which to collect data.
- Port: The port to which data is entering or leaving. This can help you narrow down traffic to a particular service.
- Port Number: The port number is important because it often indicates the reason for the traffic. For example, port 80 is the default port used for HTTP traffic.

The following example filter could be used to monitor all HTTP requests coming from one IP addresses. This filter could be used to passively monitor a suspect to see if they are using a company WLAN to access pornography:

Source IP is 192.168.1.10 AND Destination Port is 80

Note: Unless you are a law enforcement officer with a proper warrant, we do not recommend spying on your users. It is unethical and can be illegal, even if the employee is using your company network and even if you have a strict usage policy.

To setup this filter, select 'Source IP Address' from the top filter group, leave the condition as 'IS', and enter the IP address '192.168.1.10' in the value field. Then select 'AND' from the middle condition menu and select the 'Destination Port' from the lower filter group menu. Select 'IS', and enter the port number '80' in the value box.

3.1.7 Summary

Filtering is a very valuable aspect to any sniffer. For this reason we included a simple, but useful, filtering module in Airscanner Mobile Sniffer™. If used, this filter will allow you to focus on the data that matters. This will reduce the time you spend looking through the data, will reduce the wasted space filled with useless data, and will allow you to collect only data that matters to you. In addition, since this data is captured in Ethereal format, you can easily export it and analyze it much more intensely on your desktop.

3.2 Ethereal

URL: http://www.ethereal.com

Supported Platforms: Linux (RedHat, SuSE, Slackware, Mandrake), BSD (Free, Net, Open), Windows (9x/ME, NT4/2000/XP), AIX, Compaq Tru64, HP-UX, Irix, MacOS X, SCO, Solaris

3.2.1 Description

Ethereal is one of the most popular sniffers available. It performs packet sniffing on almost any platform (Unix, Windows), in both real-time (live), and from saved capture files from other sniffers (NAI's Sniffer, NetXray, tcpdump, and more). Included with this program are many features such as filtering, TCP stream reconstruction, promiscuous mode, third-party plug-in options, and the capability to recognize more than 260 protocols. Ethereal also supports capturing on Ethernet, FDDI, PPP, token ring, X-25, and IP over ATM. In short, it is one of the most powerful sniffers available on the market today—and it is free.

3.2.2 Installation on Windows

Installation varies depending on the platform. Because 98% of people using this program employ either a Linux distribution (such as RedHat) or a Windows operating system, we will be discussing only those platforms. For the most part, what works on one *nix operating system will work on another with only slight modifications to the installation procedure.

Using Ethereal with Windows is fairly straightforward. There is one exception to this point. 802.11 packet captures are not currently available using Ethereal with any Windows OS.

However, if you want to capture data from a wired network, Ethereal will work quite well.

3.2.2.1 Requirements

WinPcap: http://winpcap.polito.it

There is one requirement for Ethereal on Windows: WinPcap. This program, available for free online, enables Ethereal to link right into the network card before the data is passed up to the network software and processed by Windows. This program is required because of the way in which Windows interacts with its hardware. To reduce system crashes, any program installed in a Windows environment must interface with the OS software, which in turn communicates with the hardware. This is meant to be beneficial by restricting direct access to the hardware, which can cause software incompatibilities, ultimately resulting in system crashes.

In addition to the packet driver previously discussed, WinPcap includes another software library that can convert the captured data into the libpcap format. This format is the "standard" used by almost every *nix-based sniffer in circulation today. By incorporating this aspect into WinPcap, Ethereal can create files that can be ported to other platforms for dissection or archiving.

3.2.2.2 Installing WinPcap

To install WinPcap, follow these steps:

1. Download the file from http://winpcap.polito.it.
2. Make sure it is not already installed:
   Start →Settings → Control Panel → Add/Remove Programs
3. Run the WinPcap Install program.

3.2.2.3 Installing Ethereal

To install Ethereal, follow these steps:

1. Download the file from http://www.ethereal.com.
2. Ensure WinPcap is installed (Version 2.3 and up required):
3. Start → Settings → Control Panel → Add/Remove Programs
4. Run the Ethereal install program.
5. Select the components to install:
   - Ethereal—Standard Ethereal program
   - Tethereal—Ethereal for a TTY environment (No GUI)
   - Editcap—Tool for editing/truncating captured files
   - Text2Pcap—Tool for converting raw ASCII hex to libpcap format packet capture files
   - Mergecap—Tool for merging several capture files into one file
6. Finish installation.

3.2.2.4 Running Ethereal

Launch Ethereal from Start → Programs → Ethereal → Ethereal. Details on using the program are covered after Linux section later in this chapter.

3.2.3 Installation on Linux

Linux is the preferred platform for Ethereal. This is because Linux allows programs to

interface directly with the hardware installed in the computer. By allowing this, software writers do not have to work with poorly written or tightly managed library components, as they do in Windows. However, this increased functionality does come with its share of problems.

Because of the nature of open source software, you can never be sure what is included in a package, or how it will work with a certain piece of software. Whereas one program might work flawlessly right out of the box, another program might require several additional operating system components or tweaks to existing files before it will run. However, Ethereal is fairly stable across the various Linux platforms, as long as you ensure that the configuration file is set up correctly.

3.2.3.1 Requirements

Ethereal for Linux has several prerequisites. By meeting these requirements before you attempt to install the software, you will have a relatively easy installation process. Some of these prerequisites are not necessary for the core functionality of Ethereal; however, they will add extra features to make it more productive.

NOTE
Although each of these prerequisites does have its own home page, you can get them all from the local archive at http://www.ethereal.com.

- GTK+ and Glib (http://www.gtk.org)—This program is the de facto standard toolkit used to create GUIs in the Linux environment. Ethereal requires this program for installation.
- Libpcap (http://www.tcpdump.org)—Libpcap for Linux is required by Ethereal to facilitate the capture and formatting of the data from the NIC. Ethereal requires this program for installation.
- Perl (http://www.perl.com)—Perl is the programming language of choice for small projects in the Linux environment. Ethereal uses it to build the documentation.
- Zlib (http://www.info-zip.org/pub/infozip/zlib)—Zlib is a compression software library that can be installed with Ethereal to facilitate the reading of compressed gzip files on the fly. This program is optional for Ethereal.
- NET-SNMP (http://net-snmp.sourceforge.net)—NET-SNMP is a software library used to read and write SNMP data. Ethereal uses this optional component to decode captured SNMP data.

3.2.3.2 Installation Options

Installing Ethereal requires several steps. You should be somewhat familiar with the general installation process before attempting to perform this process. Install scripts typically request various configuration settings, such as your source directory, module directory, and more. However, for those who do not want to run through the manual building of source code, RPM files are available for download. The following briefly describes the general steps involved in installing from source code and in installing from RPM. As you can see, using the RPM is much simpler. Installing RPMs Use the following format to install RPMs. This should result in a complete install, without the need to configure or install source code.

rpm –ivh filename.version.i386.rpm

Installing Source Code

This is not recommended for the complete beginner. However, if you have customized your system or want to play with the code, or are having problems installing the RPMs, the source code is available for download. The following is the typical procedure for compiling and installing source code.

NOTE

You will need a compiler installed. The most common is gcc, which is typically available on the Linux CD.

1. Unpack the source code using the tar command:
   tar xvf file.version.tar.gz
2. cd into the newly created directory.
3. Run ./configure to set up the compiler scripts.
4. Run ./make all to make all the files.
5. Run ./make install to install the newly made files.

NOTE

At this point, you will want to restart any services using the files you just installed, or simply reboot.

RPM Installation

To install the RPMs, follow these steps:

1. Download the required files (x represents version number):

- libpcap-0.x.x-x.i386.rpm—Includes Libpcap libraries
- tcpdump-x.x.x-x.i386.rpm—Includes tcpdump libraries and program
- ethereal-base-0.x.x-1.i386.rpm—Includes base code for Ethereal
- ethereal-gnome-0.x.x-1.i386.rpm—Includes GUI code for Gnome desktop
- ethereal-gtk+-0.x.x-x.i386.rpm—Includes graphical libraries for GUI
- ethereal-kde-0.x.x-x.i386.rpm—Includes GUI code for KDE desktop
- ethereal-usermode-0.x.x-x.i386.rpm—Includes code for Ethereal

NOTE

The other source code files are found at their respective sites.

2. Install gtk+.
3. Install libpcap.
4. Install tcpdump.
5. Install ethereal-base.
6. Install ethereal-usermode.
7. Install ethereal-gnome and/or install ethereal-kde.

3.2.3.3 Common Errors

While *nix-based operating systems allow users much more flexibility, this does come with

a price. Therefore, do not be surprised if you get an error or two while installing these programs. To help, we have provided a few troubleshooting tips to ease the pain.

Missing Files and/or Directory Errors

If you receive an error relating to a file or directory that is non-existent, the problem can be solved by manually creating this directory or by creating a link to the necessary file. A Unix "link" is similar to a Windows shortcut and will satisfy the installation script and any program that needs the file.

1. Manually create the missing directory (for example, mkdir /usr/local/include/net).
2. Locate the missing file and copy it into the directory, or create a symbolic link to the file.

Missing libcrypto.0 File

This is one error that seems to be common; thus, we included specific instructions on how to correct it. The problem is related to changes in where Linux places files as it is installed.

1. Create a symbolic link to the libcrypto.0 file using an existing libcrypto.0.x file (for example, ln libcrypto.0.x libcrypto.0).
2. Install RPM using the —nodep option.

3.2.4 Running Ethereal

Ethereal can be launched from the command line (ethereal&). Details about the program are covered next.

3.2.4.1 Using Ethereal

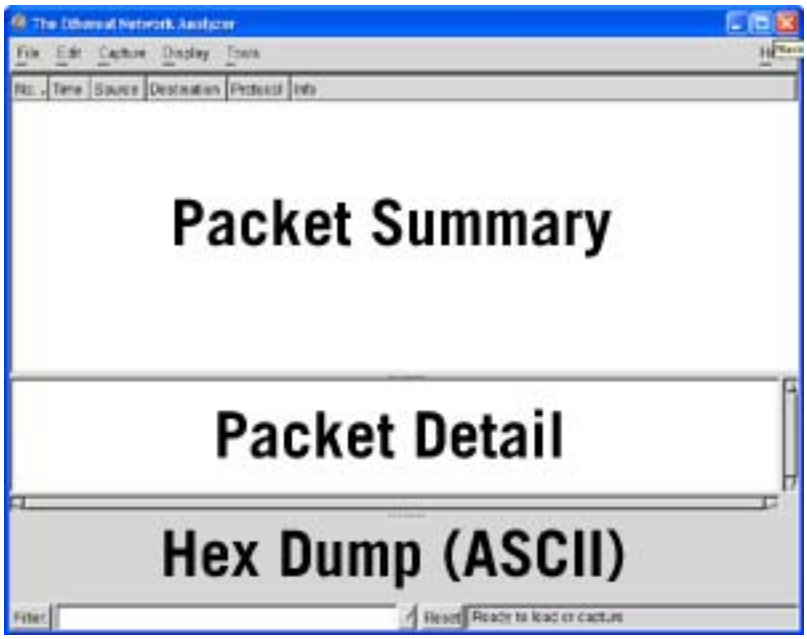
Using Ethereal is basically the same regardless of the OS. The GUI and general operation of this program is the same regardless of the platform on which it was installed, with the exception of general file menu operations. Because of the similarities, we will cover the use of the program once.

3.2.4.2 GUI Overview

After Ethereal is loaded, you will see three screens, as illustrated in Figure 9.1. Each of these frames serves a unique purpose for the user, and will present the following information.

- Packet Summary—This is a list of all the captured packets, which includes the packet number (1–65, 535), time-stamp, source and destination address, protocol, and some brief information about the data in the packet.
- Packet Detail—This window contains more detailed information about the packet, such as MAC addresses, IP address, packet header information, packet size, packet type, and more. This is for those people interested in what type of data a packet contains, but don't care about the actual data. For example, if you are troubleshooting a network, you can use this information to narrow down possible problems.
- Packet Dump (Hex and ASCII)—This field contains the standard three columns of information found in most sniffers. On the left is the memory value of the packet; the middle contains the data in hex; and the right contains the ASCII

equivalent of the hex data. This is the section that lets you actually peer into the packet and see what type of data is being transmitted, character-by-character.



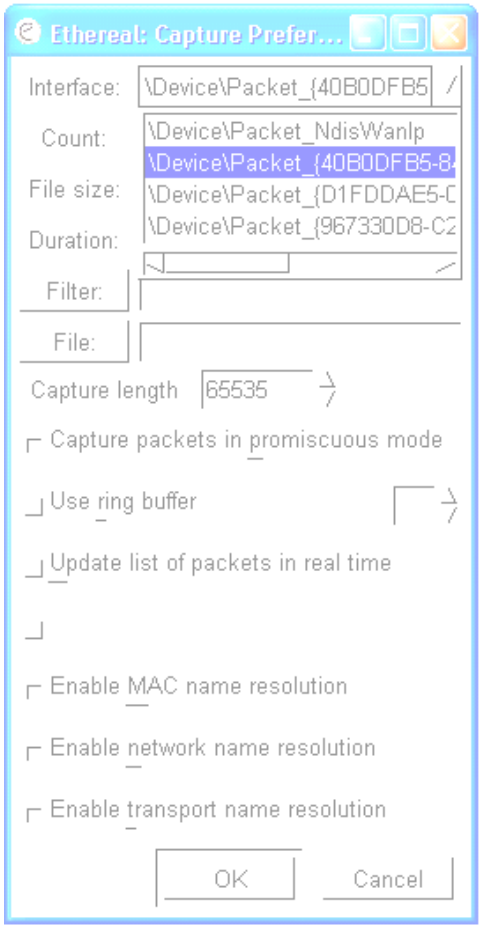
3.2.4.3 Configuration

Using Ethereal can be as simple as you want it to be. By default it comes with everything set up for full sniffing, and the only necessary setting is the selection of the network interface device. However, because of a very user-friendly user interface, this option is simple to use and easy to find.

To start sniffing, ensure that you have a network card in operational mode. This means the NIC's drivers must be installed and the card must be able to receive and transmit data. If the card does not work properly before using Ethereal, it will certainly not work while it is running. In addition, if you are using a WNIC, you might be limited as to how far out on the network you can sniff. If you are using a *nix OS, you will probably be able to sniff to at least the wireless router, wireless access point, or closest switch. If you are using Windows, your WNIC will only capture local data. Keep this in mind, or else you will spend hours attempting to troubleshoot a known issue.

To set up Ethereal to use your NIC, click Capture → Start. You will be shown a screen similar to Figure 9.2.

(C) 2003 Airscanner Corp. http://www.airscanner.com



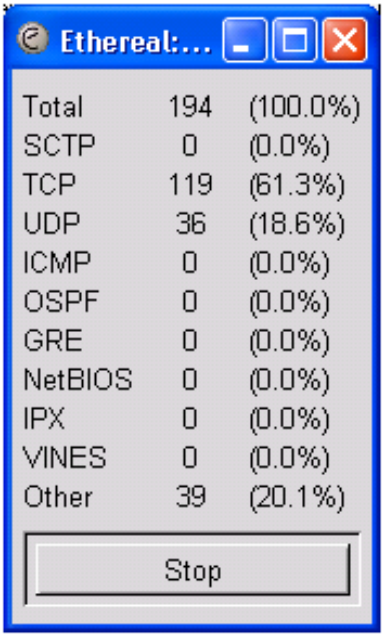
The interface option must be set to the NIC currently installed and in operation. Note that in the example there are four options available. This list is from Ethereal as it appears when installed in Windows XP. For this operating system, the list contains the NIC by MAC address. Other versions of Windows create a list by pseudo-names (for example, cw10, PPPMAC, wldel48, and so on). Linux's list, on the other hand, is by interface name (for example, wlan0, eth0, eth1,and so on).

Next, you have the capability to adjust various aspects of how Ethereal captures information. For example, you can set it up to filter the data and only capture HTTP information. Or, you can capture the data and update Ethereal's display in real time. You can also set up the ring buffer to create numerous files in case you collect the maximum number of packets required to fill up the first file (it allows you to capture infinite amounts of data). You can also adjust name resolution settings, which might speed up processing, but which might reduce valuable data if disabled.

NOTE

Using Ethereal will affect your normal network connection. If you place the NIC in promiscuous mode, you could have various connection issues.

Once these settings meet your satisfaction, click the OK button to start sniffing. After you do this, you will see a small window open up that provides you with a running tally of the number of each type of packet collected.

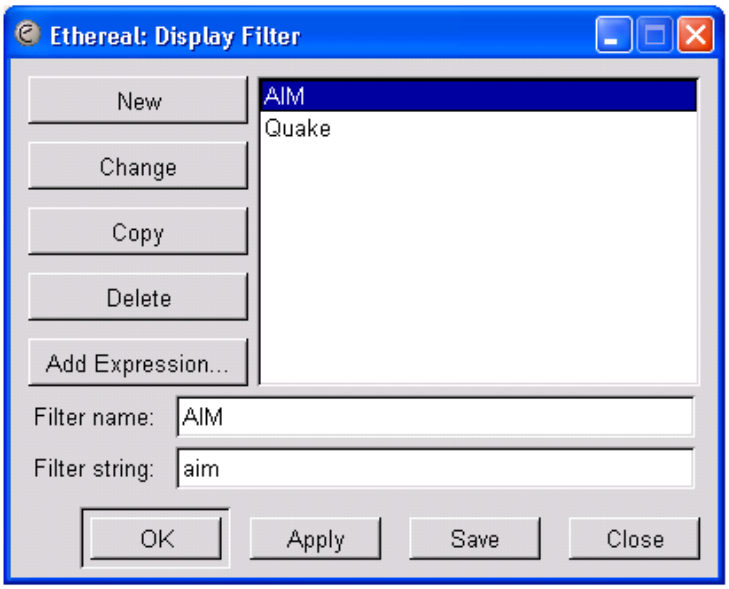


NOTE: The stats window only displays the common protocols. All others are lumped under the Other category, which will require further investigation.

3.2.4.3 Ethereal's Filter options

After you capture a significant amount of data, the next step is to filter it based on your preferences. For example, if you are looking for traffic generated by the AIM protocol, which is used by AOL's Instant Messenger, you can set up a filter to quickly parse all AIM data out of the captured data. This can also be done before the capture; however, post-capture filtering is recommended because it gives you the power to go back and review everything captured.

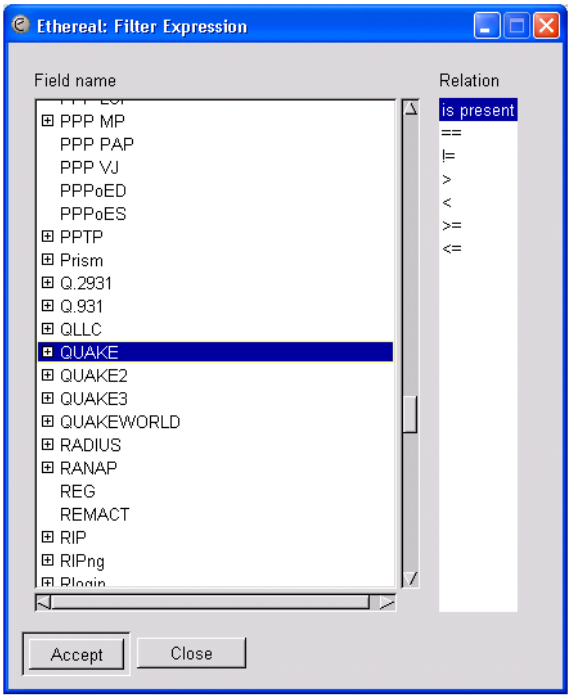
To set up a filter before the capture, use the filter option as illustrated in Figure 9.2. This will open a filter setup window similar to Figure 9.4. To post the filter, use the filter option at the bottom of the Ethereal window



In this example, we will create a filter for AIM and Quake. Quake is a multiplayer game whose mastery is an essential prerequisite for any competent security professional. However, if you are a network administrator, you might desire a way to periodically monitor your network for Quake packets to make sure no one has set up a rogue Quake server. To do this, perform the following steps:

1. Click the Filter button.
2. Type Quake in the Filter Name textbox.
3. Click the Add Expression button.
4. Scroll through the list of options and select Quake in the Field Name column and is present in the Relation column (see Figure 9.5).
5. Click Accept.
6. Click the New button to add the filter to the save list.
7. Click Save to store this filter permanently.
8. Click OK to use the filter.

This should process the data captured and parse out only those packets that include the Quake protocol. If nothing appears in the screen, or no packets are detected, Quake is not being



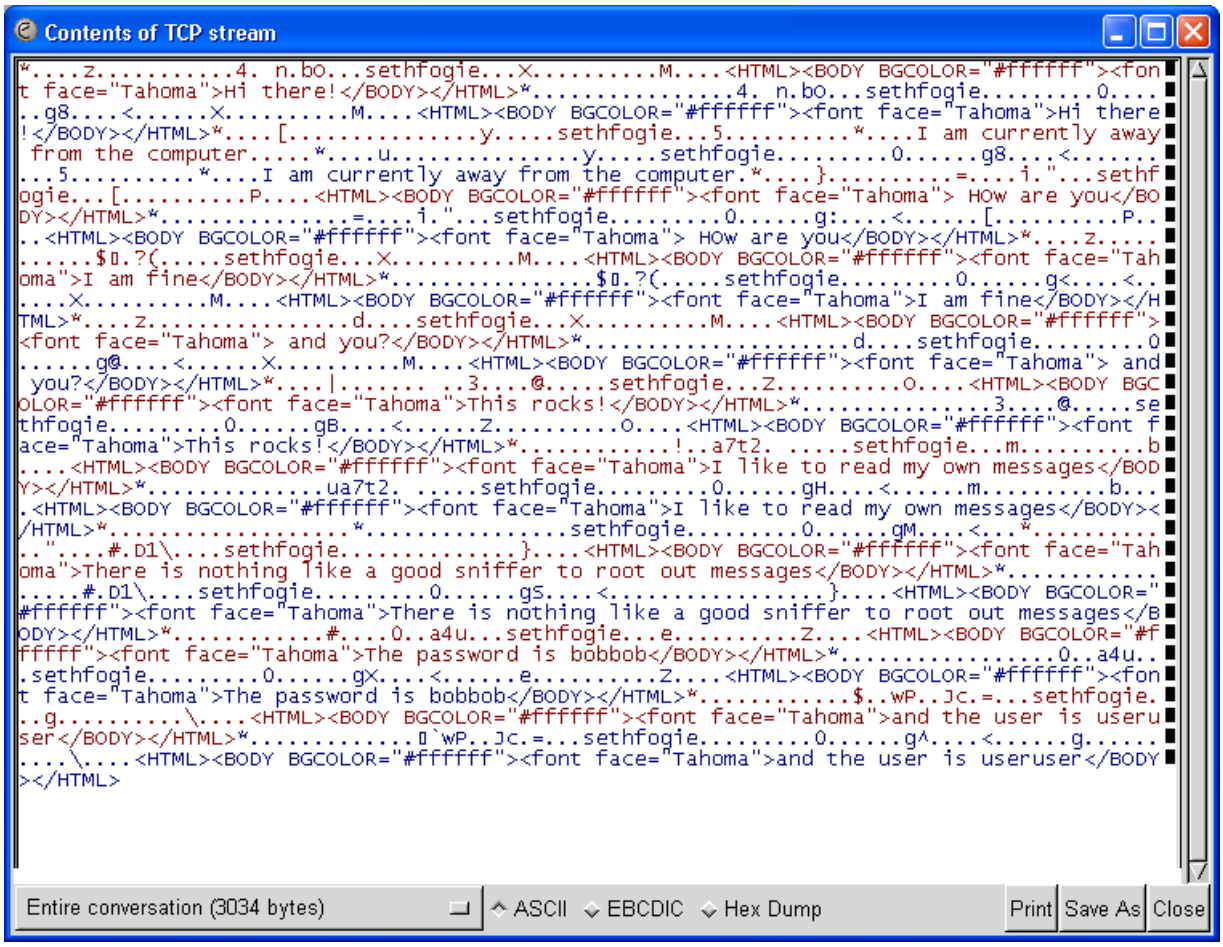
used on the network. After you are finished with this filter, click the Reset button and Ethereal will return all the captured data to the program windows.

3.2.4.4 The Follow TCP Stream Option

Ethereal comes with one outstanding feature that puts it at the top of our recommended list of sniffer programs. Besides the fact that it is free, Ethereal will also reconstruct TCP streams from the jumbled collection of data. To illustrate how useful this function is, we are going to perform a short capture while using AIM. Thus we start Ethereal and set it to listen to the

network. To facilitate this example, we simply sent messages to our own chat client. After a few sentences, we stop the capture and let Ethereal load the data into the packet display windows. At this point, we have a great deal of commingled data. How can we sort through this data to find our chat session?

We could set up a filter; however, this would still leave us with numerous packets that we would have to piece together. Because of this, we are going to use the TCP stream-following feature incorporated into Ethereal. This feature alone distinguishes Ethereal from the many others available; in addition, Ethereal is free. To use this, we need to find a packet using the AIM protocol and right-click on it. This will bring up a menu, which contains Follow TCP Stream as the first option. We click on this, and after a few seconds (or minutes, depending on the computer speed and the amount of data) we get a window similar to Figure 9.6. Now we have our complete chat session available to read through. If a hacker or network administrator were using this program while you were chatting with a friend, she too would be able to see the entire conversation.



As you can see, Ethereal has almost unlimited possibilities. It is full of features that make it the obvious choice for the both the low budget hacker or the thrifty network administrator. This is one program that should be part of every computer geek's arsenal or investigative tool bag.

4. Troubleshooting

If you experience problems with Airscanner Mobile Sniffer™, please review the following symptoms to help guide your trouble shooting efforts:

Unable to set mode. This error is given when the Mobile Scanner can's set the WNIC in promiscuous mode. This is usually caused by the use of an unsupported WNIC or improper drivers.

Error opening this adapter. Please "soft" reset your device and select another adapter. This error is given if the selected adapter is not

5. Summary

Airscanner Mobile Sniffer™ is a necessary component to any administrator's toolkit. Included in this program are several useful functions and features that make it easy to use and user-friendly. Filtering, packet details, and a statistical breakdown all help you manage and monitor your WLAN traffic effectively and efficiently. In addition to a useful analysis of data on the Pocket PC, Airscanner Mobile Sniffer™, saves data in Ethereal format, which allows further analysis of a capture session from your desktop. This can allow you to rebuild web pages, emails, and perform in depth analysis of all data captured.

6.FAQs

General FAQ:

How do I get technical support?

Free (personal, non-commercial) versions are not directly supported. Your first level of support is this user's manual. In addition, you can often find help from Airscanner developers and other helpful users on our web forum at www.airscanner.com.

Paid licensees receive prompt and courteous email support for the duration of their license. Optional support packages are also available for corporate users who require flexible levels of support.

Why is Airscanner™ software free for personal use?

Providing Airscanner software free for personal use allows us to gain market share. We are not blindly driven by profits; instead, our primary goal is to have everyone in the world happily using Airscanner software. We have found that users who download the free version like it so much that they recommend it to their friends and family… and they in turn like it so much they often buy licensed copies for work. There has never been, nor will there ever be, hidden spyware or "ad-ware" in any Airscanner software.

When do I have to pay for Airscanner™ software?

Corporate, Educational, Government, and Small Business/Home Office users must purchase an annual license within 30 days of installing the software. Please take the full 30 days to evaluate the software to ensure compatibility before purchasing a license. It is illegal to use Airscanner™ software beyond 30 days for business use without a paid license.

What is the difference between the freeware and paid versions?

There is no difference between the freeware and paid versions of Airscanner™ software. In fact, they are the same. The difference is in the use and licensing: the software is free for personal use, but you are required to pay for a license if you use it for business.

I am considering buying a license, but first I need help getting it to work. Can I get free support? I promise I'll buy it if it works.

Unfortunately, the most expensive part of software development is support. We have tens of thousands of new users every month. If we tried to support the freeware or shareware versions we would quickly go out of business. Thus, we can only provide support to those who have paid for a license. However, please do try to get help from other friendly users on the unofficial help forum linked from our website.

(C) 2003 Airscanner Corp. http://www.airscanner.com

Software-specific FAQ:

Is my network card supported?

Airscanner™ Mobile Sniffer supports all known wireless networking cards and integrated WiFi such as the Toshiba e740 series -- and even the flawed IPAQ 5450 series to some extent (use the fix below to correct the reported problems in the 5450 hardware). They key is to select the correct adapter at program start-up. Please check with your device manufacturer to find out what the appropriate driver name for your card is. Note certain footnotes and exceptions to this as described below.

Does your product work with the IPAQ 5450 series?

Latest Update: HP has partially fixed their 5450 wireless hardware problem in a later ROM release (1.11.19 ROM). If you download this fixed version of the ROM or later from HP, you will be able to view packets non-promiscuously by choosing the correct adapter (vnetusba1), without having to perform the registry hack listed below. However, you will need to reset your device for each new capture session. Hopefully HP will continue to work on their bug in the 5450 series drivers. Thanks to Benjamin Bolton for this update.

Yes, it works with the 5450 series. Part of the problem is mistakes from your device manufacturer.[1] In the meantime, Sgyee, a reviewer for PDAJunkie.NET, offers this hack on how to get the sniffer working on the IPAQ 5450:

1) Load the ROM Update
2) Load the WLAN update over the ROM update
3) Perform the VNETMINI1 registry patch (see below)
4) Load AirScanner Mobile Sniffer
5) Turn off promiscuous mode.

How to perform the VNETMINI1 registry patch:

To fix HP's error in order to enable your WLAN card so programs like Airscanner Mobile Sniffer can see it, use a CE registry editor to go to

\HKLM\Comm\vnetmini\Linkage

Then delete the Multi-String Value Route and enter a new Multi-String Value Route with the value of vnetmini1.

---

[1] *See "How to Hack your 5455 to fix the things HP broke" Forum post by David Hettel, Feb. 18, 2003. http://www.wormholecreations.com.au*

Note that this method works only in non-promiscuous mode.

Does your product work on the Toshiba e740 series?

Yes, it works fine on the Toshiba e740 series, including promiscuous mode. As pointed out by Dataworm of PocketWarrior, you have to select the network adapter named **EC2NDS1**. Either select this adapter at program startup, or go to **Options→Select Adapter** from the program's main screen.

If it works fine with the Toshiba e740 series, why not the e750?

Our sniffer should actually work with any adapter, since ours is just an ethernet sniffer with no inherent WiFi capability, unlike programs like netstumbler or pocket warrior (to which we have contributed free source code). We currently have tens of thousands of users of our sniffer, but only a handful of driver conflicts. However, sometimes your hardware device manufacturer unintentionally "breaks" the functionality of its WiFi adapter for 3rd party programs. A good example of this is the IPAQ 5450 series, which is the sister device of the Toshiba. Finally, someone figured out a special registry hack to fix the functionality that HP "broke" in their PDA. HP has also started to fix their hardware problem in later ROM updates. The Toshiba e740 adapter works perfectly, so presumably there is a problem (or limitation) with the newer driver for e750 that prevents it from working with certain 3rd party programs. We have notified Toshiba of the issue. Make sure to try a soft reset first, and make sure to disable other WiFi programs. If it still doesn't work, your best bet is to wait for a working driver or ROM update from HP or Toshiba.

Does your Airscanner Mobile Sniffer work on older devices running PocketPC 2000, such as my Jordana or Casio E-125? If not, do you have any plans to offer a product that will work with PocketPC 2000 in the future?

Our products only support PocketPC 2002/2003 running on devices with ARM-based processors (including X-scale), which is the most prevalent platform. We unfortunately cannot support older operating systems or devices.

I don't see any packets? Is it working?

While the mobile sniffer will pick up most packets, if the data is transmitted from a 'hidden' WLAN, it will not be detected. In addition, you will need to enable the Promiscuous Mode under the Options menu. Without this enabled, you will only be able to pick up traffic sent to or from your own Pocket PC.

I get a "Can't Set Mode" error?

This could possibly be resolved by a driver update, if you are using incorrect drivers for your WNIC.

(C) 2003 Airscanner Corp. http://www.airscanner.com

What can I do with the data I collect?

Mobile Sniffer is a great first level tool. It can provide instant access to important data; however, it is not a full-fledged analyzer. We recommended you try Ethereal for a deeper analysis, which is why our saved files are in this format. Ethereal is free and available at www.ethereal.com. It works wonderfully with Airscanner Mobile Sniffer packet session captures.

I just saw my user name and password in a sniff session! Is this normal?

YES! This is why any wireless network MUST be encrypted. Email, instant messages, web pages, and other tidbits of data are easily captured and read by a network. If you can see your personal information on your WLAN, so can anyone else.

Can anyone tell that I am sniffing?

There are tools available online that can help a person deduce that a sniffer is in operation. However, due to the fact that wireless is broadcasted, a passive sniffer can usually capture everything without being detected.

Winpcap is Copyright (c) 1999-2003 NetGroup, Politecnico di Torino. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the *"Politecnico di Torino"* nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.